Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ТЕХНОЛОГИИ КАНАЛЬНОГО УРОВНЯ МОДЕЛИ OSI В GNS3»

Выпускная квалификационная работа бакалавра
по направлению 44.03.04 Профессиональное обучение (по отраслям)
профиля «Энергетика»
профилизация «Компьютерные технологии автоматизации и управления»

Идентификационный код ВКР: 127

Екатеринбург 2016

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ Н. С. Толстова
«____» _____ 2016 г.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ТЕХНОЛОГИИ КАНАЛЬНОГО УРОВНЯ МОДЕЛИ OSI В GNS3»

Выпускная квалификационная работа бакалавра
по направлению 44.03.04 Профессиональное обучение (по отраслям)
профиля «Энергетика»
профилизация «Компьютерные технологии автоматизации и управления»

Идентификационный номер ВКР: 127

Исполнитель:
студент группы КТэ -401 В. Е. Паньшин
Руководитель:
ст. преподаватель С. С. Венков
Нормоконтролер: Т. В. Рыжкова

Екатеринбург 2016

РЕФЕРАТ

Пояснительная записка к выпускной квалификационной работе выполнена на 52 страницах, содержит 17 рисунков, 30 источников информации.

Ключевые слова: АГРЕГИРОВАНИЕ КАНАЛОВ, RPVST+, ВИРТУАЛЬНАЯ ЛОКАЛЬНАЯ СЕТЬ, NATIVE VLAN.

Объект — процесс обучения настройке технологий канального уровня модели OSI в рамках дисциплины «Компьютерные коммуникации и сети».

Предмет — учебные материалы дисциплины «Компьютерные коммуникации и сети».

Цель работы — разработать лабораторный практикум по настройке и использованию технологий канального уровня модели OSI в GNS3.

Для достижения поставленной цели были решены следующие задачи:

1. Проведен обзор и анализ литературных и интернет-источников.
2. Рассмотрены программные симуляторы для построения и настройки схем компьютерных сетей.
3. На основе анализа рабочей программы дисциплины «Компьютерные коммуникации и сети» спроектированы лабораторные работы.
4. Спроектированные работы объединены в методические указания к лабораторным работам и реализованы в формате .pdf.

Результаты выпускной квалификационной работы будут использоваться для проведения занятий по дисциплине «Компьютерные коммуникации и сети» в Российском государственном профессионально-педагогическом университете г. Екатеринбург.

СОДЕРЖАНИЕ

Введение 4

1 Обзор аппаратного и программного обеспечения технологий канального уровня модели OSI 6

1.1 Обзор и анализ литературы и интернет-источников 6

1.2 Симуляторы для построения и настройки компьютерных сетей ... 7

1.3 Обзор коммутационного оборудования компании Cisco System . 13

1.4 Протоколы канального уровня 20

2 Методические указания к Лабораторным работам по теме «Технологии канального уровня модели OSI в GNS3» 36

2.1 Структура и программная среда разработки лабораторного практикума 37

2.2 Описание лабораторных работ лабораторного практикума «Технологии канального уровня модели OSI в GNS3» 40

Заключение 48

Список использованных источников 49

Приложение 52

ВВЕДЕНИЕ

Повсеместная компьютеризация является неотъемлемой частью современной жизни. На текущий день практически любая сфера жизни невозможна без применения того или иного компьютеризированного устройства. Это способствует увеличению числа компьютеров и усложнению взаимосвязей между ними. Для упрощения взаимодействия компьютеров их объединяют в сети. Эти сети нужно уметь настраивать. Отсюда возникает потребность в повышение качества профессионального образования и уровня подготовки компетентных, творческих и высококвалифицированных специалистов, соответствующих требованиям социального заказа общества.

Поскольку не всегда есть возможность обеспечивать учебные заведения дорогостоящим оборудованием ведущих фирм, на помощь приходят симуляторы, позволяющие обучить специалистов работе на самом современном и лучшем оборудовании без привлечения дополнительных ресурсов. Достигнуть данную цель позволяет учебно-методическое обеспечение совместно с программой GNS3. Преимущество GNS3 перед другими симуляторами заключатся в том, что в GNS3 поддерживаются все функции как на реальном оборудовании. Самое интересное в GNS3 является возможность соединения проектируемой сети с реальной сетью. Это дает уникальную возможность проверить на практике какой-либо проект, без использования реального оборудования. Использование WireShark позволяет провести мониторинг трафика внутри проектируемой сети, что дает дополнительную информацию для понимания изучаемых технологий.

Объект — процесс настройки технологий канального уровня модели OSI.

Предмет — учебные материалы дисциплины «Компьютерные коммуникации и сети».

Цель работы — разработать лабораторный практикум по настройке и использованию технологий канального уровня модели OSI.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести обзор и анализ литературных и интернет-источников.
2. Рассмотреть программные симуляторы для построения и настройки схем компьютерных сетей.
3. На основе анализа рабочей программы дисциплины «Компьютерные коммуникации и сети» спроектировать лабораторные работы.
4. Спроектированные работы объединить в методические указания к лабораторным работам и реализовать в формате .pdf.

1 ОБЗОР АППАРАТНОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЙ КАНАЛЬНОГО УРОВНЯ МОДЕЛИ OSI

1.1 Обзор и анализ литературы и интернет-источников

Перед выполнением работы был изучен и проанализирован ряд учебных изданий, а также иные учебные материалы по теме работы.

Книга «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101» содержит исчерпывающие теоретические знания по работе на оборудовании Cisco. Единственный недостаток — это проблемы с переводом. Присутствуют ошибки и опечатки.

Электронный ресурс learningnetwork.cisco.com охватывает все возможные темы. Содержит проверенную и самую свежую информацию. Недостаток — все материалы на английском языке.

Сайт xgu.ru электронная вики-энциклопедия, описывающая в основном IT-технологии и администрирование компьютерных систем — большой охват тем и хорошее содержание по работе с оборудованием Cisco.

Электронный ресурс www.cisco.com — наиболее актуальный источник информации. Сайт охватывает все этапы работы с оборудованием Cisco, поддерживает множество языков, оперативно обновляется в соответствии с изменением в ПО или оборудовании компании.

Печатное издание CCNA 640-802 Official Cert Library, Updated, 3rd Edition. Эти книги — официальное руководство по подготовке к экзамену CCNA. Рассматривается большое количество актуальных тем. Выпускаются только на английском языке.

Книга Тодда Леммла CCNA Cisco Certified Network Associate Study Guide, 7th Edition. Если сравнивать с изданиями, описанными выше, то мож-

но сказать что в этом издании информация более живая и воспринимается легче. Но также издается на английском языке.

Видео-руководство от CBT Nuggets, — cbtnuggets.com. Не распространяется бесплатно и все ролики на английском языке.

Ресурс ciscolab.ru, содержит много полезной информации. Здесь можно найти русскоязычные статьи и книги, но англоязычные преобладают.

Форум и сайт sadikhov.com и sadikhov.com/forum многие годы был и остается местом обсуждения интересных тем IT-профессионалов в самых различных областях и здесь можно найти много полезной информации.

Рабочая программа дисциплины «Компьютерные коммуникации и сети» находится в разработке. Поэтому велись консультации с ведущим преподавателем, чтобы не использовать устаревшую версию рабочей программы.

1.2 Симуляторы для построения и настройки компьютерных сетей

Существует множество симуляторов для построения и настройки компьютерных сетей. Рассмотрим некоторые из них:

- UNetLab;
- Cisco packet tracer;
- GNS3.

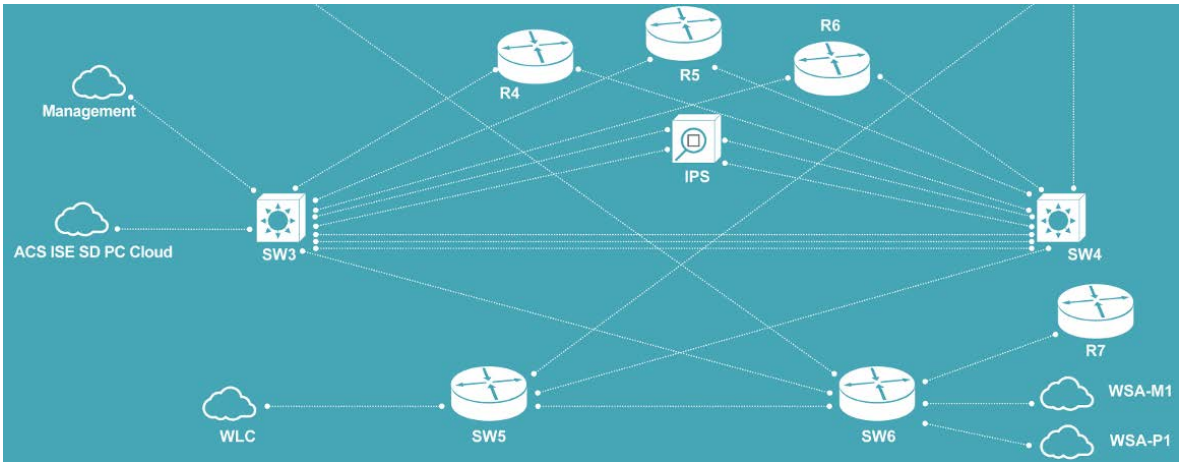

Рисунок 1 — UNetLab

UNetLab — (Unified Networking Lab, UNL) это мульти-вендорная и многопользовательская платформа для создания и моделирования самых различных лабораторий и дизайнов, которая позволяет смоделировать виртуальную сеть из маршрутизаторов, коммутаторов, устройств безопасности и др.

Это продолжение того же девелопера, который в своё время создал веб фронтенд для IOU. Теперь разработка iou-web завершена, разрабатывается только UNetLab и является незаменимым инструментом для подготовки к CCIE, сетевого инженеринга, в том числе и Troubleshooting.

UnetLab — полностью бесплатен. Вы можете запускать столько экземпляров оборудования (роутеров, коммутаторов, устройств безопасности и т.д.) сколько вы хотите и какого хотите. Например, в том же Cisco VIRL Personal Edition вы ограничены 15-ю узлами и набор устройств довольно скромный. Например, полноценную ASA получить не представляется возможным, равно как и маршрутизатор с Serial-интерфейсом.

Поддержка оборудования в UNetLab очень широкая. Вы можете запускать Cisco IOL-образы, образы из VIRL (vIOS-L2 и vIOS-L3), образы ASA Firewall (как портируемые 8.4(2), 9.1(5), так и официальные ASAv), образ Cisco IPS, образы XRv и CSR1000v, образы dynamips из GNS, образы Cisco

vWLC и vWSA, а также образы других вендоров, таких как Juniper, HP, Checkpoint и т.д.

Кроме того, начиная с версии UNetLab 0.9.54 появился многопользовательский функционал. На одной и той же VM, каждый авторизованный пользователь может создавать свои стенды независимо друг от друга, а также совместно работать с общим стендом, который разделяют несколько пользователей одновременно. При этом пользователи запускают общий стенд независимо друг от друга.

На текущий момент поддерживаются следующий список оборудования:

- Aruba ClearPass;
- Alcatel 7750 SR;
- Arista vEOS;
- Brocade Virtual ADX;
- Citrix Netscaler VPX virtual;
- Checkpoint Firewall;
- Cisco ASA (porting);
- Cisco ASAv;
- Cisco CSR 1000V;
- Cisco IPS (porting);
- Cisco IOS 1710/3725/7206 (dynamips, ethernet only);
- Cisco IOL (for Cisco internal use only);
- Cisco NX-OSv – titanium (for VIRL customers only);
- Cisco vIOS (for VIRL customers only);
- Cisco vIOS L2 (for VIRL customers only);
- Cisco XRv;
- Cisco WSA virtual appliance;
- Cisco Wireless controller – vwlc;

- Extreme Networks virtual;
- F5 BIG-IP LTM VE;
- Fortinet FortiGate (new);
- HP VSR1000;
- Juniper Olive (porting);
- Juniper Networks vMX router;
- Juniper vSRX;
- Palo Alto VM-100 Firewall;
- VyOS;
- MS Windows hosts;

Самые существенные плюсы UnetLAB:

- полностью бесплатен;
- практически полноценная поддержка L2 (за счет EOS-коммутатора, который полностью cisco-like);
- широкая поддержка Cisco оборудования;
- число запускаемых узлов ничем не ограничено, кроме ваших ресурсов (CPU, RAM);
- мультивендорность;
- многопользовательский функционал;
- низкие требования к ресурсам ПК.

Данная платформа подойдет как новичкам для подготовки к CCNA/CCNP, так и профессионалам для подготовки CCIE Routing and Switching, CCIE Security, CCIE Service Provides, CCIE Data Centers и т.д, а также для других разнообразных инженерных задач.

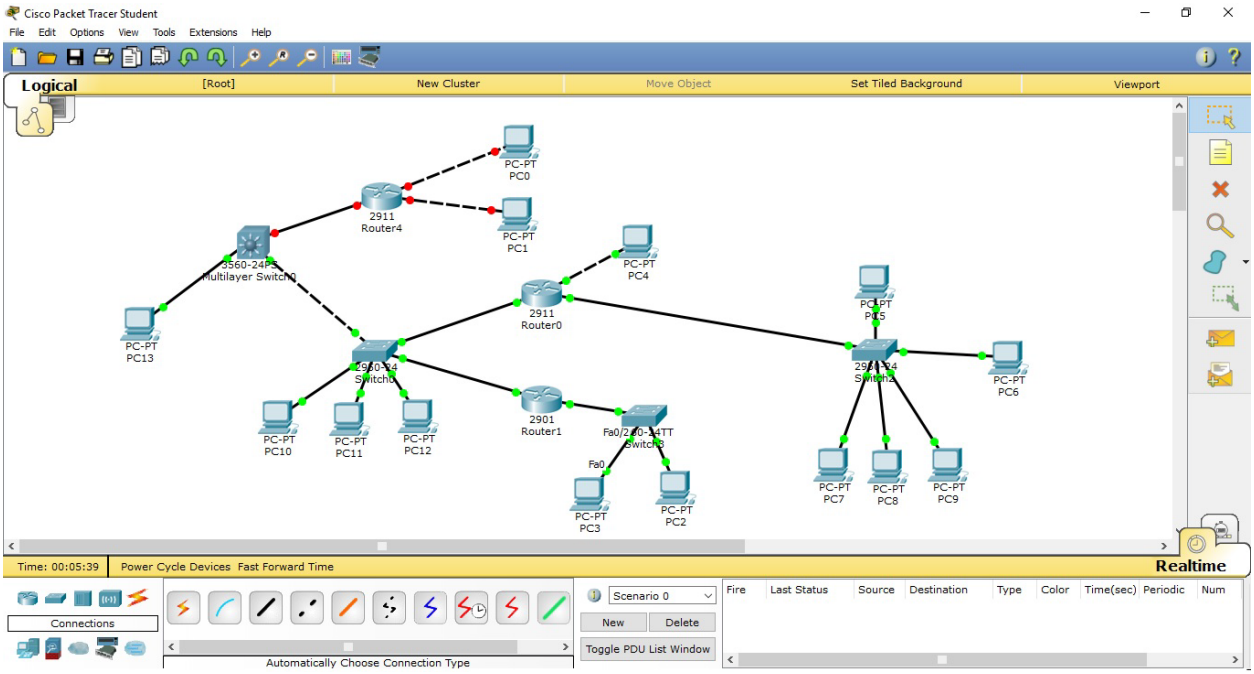

Рисунок 2 — Cisco packet tracer

Cisco packet tracer — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями (через облако). В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IP-фоны, смартфоны, хабы, а также облако, эмулирующее WAN. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары.

Успешно позволяет создавать даже сложные макеты сетей, проверять на работоспособность топологии. Однако, стоит заметить, что реализованная функциональность устройств ограничена и не предоставляет всех возможностей реального оборудования.

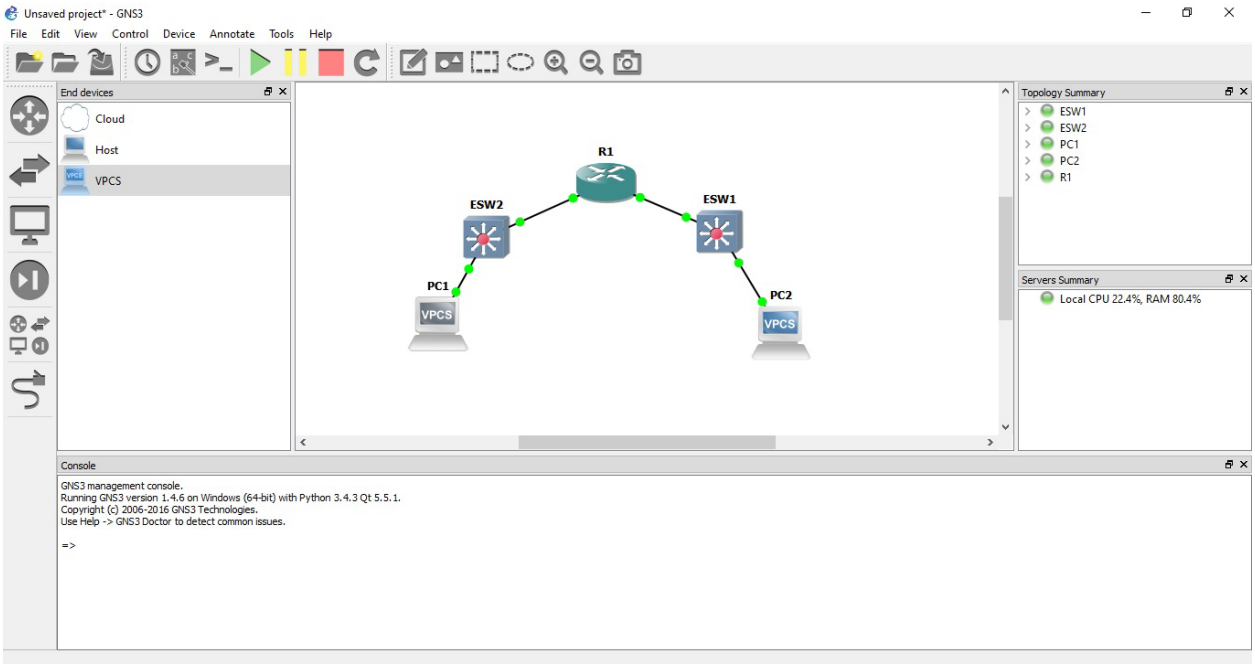

Рисунок 3 — GNS3

GNS3 — Graphical Network Simulator — это графический симулятор сети, который позволяет смоделировать виртуальную сеть из маршрутизаторов и виртуальных машин. Незаменимый инструмент для обучения и тестов. Работает практически на всех платформах. Отлично подходит для создания стендов на десктоп машинах.

В зависимости от аппаратной платформы, на которой будет использоваться GNS3, возможно построение комплексных проектов, состоящих из маршрутизаторов Cisco, Cisco ASA, Juniper, а также серверов под управлением сетевых операционных систем. При отсутствии возможности получить доступ к реальному оборудованию, GNS3 станет практически полноценной лабораторией. Кроме того, лабораторные работы, выполняемые в GNS3, могут стать дополнением к занятиям в реальной лаборатории.

Единственным недостатком данного программного обеспечения является отсутствие возможности полноценной симуляции коммутаторов второго уровня Cisco. Этот недостаток не будет исправлен в новых версиях, так как его причиной является кардинальное различие в аппаратной платформе маршрутизаторов и свитчей Cisco. В некоторых случаях данный недостаток получается обойти при помощи сетевого модуля NM-16ESW. К сожалению, листинг команд немного отличается в случае использования NM-16ESW и реальных свитчей Cisco, но вполне подходит для обучения.

В состав GNS3 не входят образы IOS/IPS/PIX/ASA/JunOS, так как они являются частью коммерческих продуктов соответствующих компаний, и никакого прямого отношения к проекту GNS3 не имеют. На данный момент это уже не является проблемой, так как найти необходимый образ уже не составляет труда.

Одной из самых интересных особенностей GNS3 является возможность соединения проектируемой топологии с реальной сетью. Это дает просто уникальную возможность проверить на практике какой-либо проект, без использования реального оборудования. Использование WireShark позволяет провести мониторинг трафика внутри проектируемой топологии, что дает дополнительную информацию для понимания изучаемых технологий.

GNS3 абсолютно бесплатен. Это открытое программное обеспечение, и любой желающий может скачать его с официального сайта проекта в разделе Download. На данный момент есть версии для Linux, MS Windows XP и Windows 7, а также для MacOS.

1.3 Обзор коммутационного оборудования компании Cisco System

Cisco (произносится «сиско») — американская транснациональная компания, разрабатывающая и продающая сетевое оборудование, предназна-

ченное в основном для крупных организаций и телекоммуникационных предприятий.

Одна из крупнейших в мире компаний, специализирующихся в области высоких технологий. Изначально занималась только корпоративными маршрутизаторами.

Cisco — мировой лидер в области сетевых технологий, меняющих способы человеческого общения, связи и совместной работы. Деятельность компании сосредоточена на пяти основных технологических направлениях: магистральная маршрутизация, коммутация и услуги; решения для совместной работы; виртуализация центров обработки данных и облачные вычисления; видеотехнологии; архитектуры для трансформации бизнеса. Чистый объем продаж компании в 2013 финансовом году составил 48,6 млрд долларов.

Компания Cisco была основана в декабре 1984 г. группой сотрудников Стэнфордского университета. Свой первый продукт компания выпустила в 1986 г. Штаб-квартиры Cisco расположены в городах Сан--Хосе (Калифорния), Амстердаме (Нидерланды) и Бангалоре (Индия).

Решения Cisco используются в основных отраслях российской экономики: в машиностроении, металлургической и нефтегазовой промышленности, в строительстве и недвижимости, розничной торговле, банках, инвестиционных и страховых компаниях.

Рисунок 4 — Маршрутизатор Cisco 7200

Router Cisco 7200 — Маршрутизаторы Cisco серии 7200 являются наиболее распространенными универсальными решениями для агрегации сервисов.

Устройства обладают следующими возможностями:

- превосходное соотношение цена/качество: Новый процессор NPE-G2 Network Processing Engine обеспечивает агрегацию сервисов на скоростях до 2 млн. пакетов/с;
- широкий набор поддерживаемых соединений, легкость в обслуживании и управлении;
- увеличенная производительность виртуальных частных сетей (VPN) благодаря новому адаптеру сервисов VPN;
- увеличенная масштабируемость и гибкость благодаря новой карте адаптера портов.

Преимущества:

- граничный сегмент распределенных сетей: Отмеченная наградами производительность системы управления качеством обслуживания (QoS);
- агрегация широкополосных сетей: До 16 000 сессий PPP для каждого шасси;
- мультипротокольная коммутация на основе меток (MPLS): Наиболее популярный выбор для реализации граничных сегментов сетей провайдеров услуг;
- виртуальные частные сети на базе IPsec: Масштабируется до 5 000 туннелей для каждого шасси;
- устанавливаемое у клиента оборудование (CPE) высшего уровня;
- поддержка шлюзов IP-to-IP: Обеспечивает точку взаимодействия между сетями сигнализации (H.323, SIP), средами передачи, трансляцию адресов и номеров портов (обеспечение конфиденциальности и скрытие топологии), функции тарификации и нормализации записей о вызовах (CDR), а также управления пропускной способностью (маркировка системы управления качеством обслуживания с использованием TOS);
- интеграция передачи голоса, видео и данных: Шасси VXR и адаптеры голосовых портов с поддержкой TDM;
- модульная архитектура: Форм-фактор 3RU и широкий набор гибких модульных интерфейсов (от DS0 до OC-3);

гибкость: поддержка Fast Ethernet, Gigabit Ethernet, Packet over SONET и др.

Таблица 2 — Технические характеристики

Оперативная память	
Память процессорного модуля	1 Гб (расширяемо до 2 Гб)
Флэш-память PCMCIA	48-128 Мб для контроллеров ввода/вывода; 64-256 Мб для процессорного модуля NPE-G2.
Флэш-память Compact Flash	256Мб
Размеры	13,34 x 42,67 x 43,18 см
Вес	22,7 кг

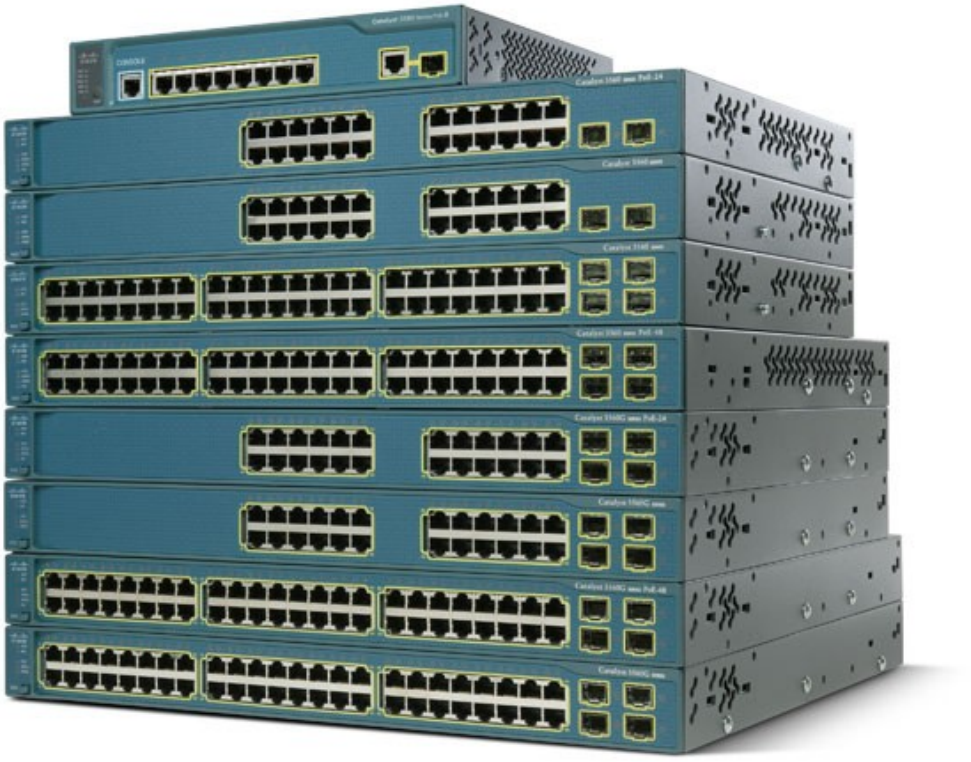

Рисунок 5 — Коммутатор Cisco Catalyst 3560

Switch Cisco Catalyst 3560 — это линейка коммутаторов корпоративного класса с фиксированной конфигурацией (в конфигурациях Fast Ethernet и Gigabit Ethernet предусмотрено питание устройств по витой паре (PoE), совместимое со спецификацией IEEE 802.3af и до-стандартным вариантом Cisco). Они предназначены для локальных сетей небольших предприятий или удаленных офисов и отлично подходят на роль коммутатора сети доступа. Эти коммутаторы уровня доступа идеально подходят для локальных сетей доступа предприятий и филиалов. Благодаря поддержке портов 10/100/1000

Мбит/с и технологии PoE, превосходной производительности и защите инвестиций, устройства позволяют развертывать новые приложения, такие как IP-телефония, беспроводной доступ, видеонаблюдение, системы управления зданиями, а также пункты удаленного обслуживания с видеосвязью.

Оборудование позволяет сохранить простоту традиционной коммутации локальных сетей и при этом развернуть интеллектуальные сетевые сервисы, такие как:

- мощная система управления качеством обслуживания (QoS);
- ограничение скорости передачи данных;
- списки контроля доступа (ACL);
- управление мультивещанием;
- высокопроизводительная IP-маршрутизация.

Основные преимущества моделей семейства коммутаторов Cisco Catalyst 3560 Series:

1. Технология PoE (Power over Ethernet) позволяет одновременно передавать по витой паре данные и обеспечивать питанием конечные устройства, например, IP-телефоны или беспроводные точки доступа Cisco Aironet.

2. Высокоскоростная маршрутизация трафика: благодаря технологии скоростной пересылки Cisco Express Forwarding (CEF) серия Cisco Catalyst 3560 обеспечивает высокопроизводительную маршрутизацию IP-трафика. SMI поддерживает статическую маршрутизацию, динамическую маршрутизацию по протоколам RIPv1 и RIPv2, а EMI — дополнительно поддерживает протоколы маршрутизации OSPF, IGRP, EIGRP, а также маршрутизацию широковещательного трафика (PIM, DVMRP, IGMP snooping).

3. Высокая безопасность: поддержка протокола 802.1x, функциональность Identity-Based Networking Services (IBNS), списки доступа для трафика, коммутируемого на канальном уровне (VLAN ACL), на сетевом и транспортном уровнях (Router ACL), а также Port-based ACLs (PACL) и Time-based ACL.

4. Расширенное управление QoS: классификация трафика по полям DSCP или 802.1p (CoS), стандартные и расширенные списки доступа для выделения заданного типа трафика, механизм контроля перегрузок очереди (Weighted Random Early Detection, WRED), механизм приоритезации трафика Strict Priority, механизм обработки очереди Shaped Round Robin. Существует возможность определения максимальной полосы пропускания для определенного вида трафика, а также выделения гарантированной скорости CIR.

5. Асинхронные потоки данных легко управляются при помощи механизмов входящего контроля (ingress policing) и ограничения трафика (egress shaping).

6. До 64 общих или индивидуальных политик на порт.

7. Поддержка системы избыточного питания Cisco Redundant Power System 675.

8. При использовании приложения Cisco Network Assistant упрощается настройка, обновление программного обеспечения и поиск неисправностей коммутатора.

9. Поддержка технологии автоматической настройки портов коммутатора под соответствующий тип кабеля (Auto-MDIX).

10. Использование динамического рефлектометра (TDR) для диагностики и выявления проблем с СКС на медных портах.

11. Поддержка протокола IEEE 802.1w Rapid Spanning Tree Protocol 802.1x с назначением виртуальной сети на пользователя.

12. Возможность создания ACL по портам для интерфейсов канального уровня, фильтрация по MAC-адресам.

13. Поддержка протокола удаленного управления и передачи файлов SSHv2 и простого протокола управления связью SNMPv3.

14. Поддержка передачи данных в обоих направлениях на порту при помощи анализатора коммутируемых портов (SPAN — Switched Port Analyzer)

15. Уведомления о новых MAC-адресах в сети.

16. Динамическое назначение виртуальных ЛВС через внедрение правил принадлежности к виртуальной сети VLAN Membership Policy Server (VMPS).

17. Протокол синхронизации внутренних часов подключенных компьютеров (Network Timing Protocol, NTP).

18. Настраиваемый размер максимального блока передачи информации (MTU) до 9000 байт, с максимальным размером фрейма 9018 байт (Jumbo frames) для бриджинга на портах Gigabit Ethernet, и до 1546 байт для бриджинга MPLS-фреймов на портах 10/100 и 10/100/1000.

19. В моделях с портами под SFP поддерживаются следующие типы интерфейсов:

- 1000BASE-SX;
- 1000BASE-LX/LH;
- 1000BASE-ZX;
- CWDM-SFP.

1.4 Протоколы канального уровня

Канальный уровень (от англ. Data Link layer) — второй уровень сетевой модели OSI, предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети. Также может использоваться для обнаружения и, возможно, исправления ошибок, возникших на физическом уровне. Примерами протоколов, работающих на канальном уровне, являются: EtherChannel, VLAN, STP.

Канальный уровень отвечает за доставку кадров между устройствами, подключенными к одному сетевому сегменту. Кадры канального уровня не пересекают границ сетевого сегмента. Функции межсетевой маршрутизации и глобальной адресации осуществляются на более высоких уровнях модели

OSI, что позволяет протоколам канального уровня сосредоточиться на локальной доставке и адресации.

Протокол EtherChannel

EtherChannel — технология агрегации каналов, разработанная компанией Cisco Systems. Агрегирование каналов (англ. link aggregation) — технологии объединения нескольких параллельных каналов передачи данных в сетях Ethernet в один логический, позволяющие увеличить пропускную способность и повысить надёжность. В различных конкретных реализациях агрегирования используются альтернативные наименования: транкинг портов (англ. port trunking), связывание каналов (link bundling), склейка адаптеров (NIC bonding), сопряжение адаптеров (NIC teaming).

LACP (англ. link aggregation control protocol) — открытый стандартный протокол агрегирования каналов, описанный в документах IEEE 802.3ad и IEEE 802.1aq. Многие производители для своих продуктов используют не стандарт, а патентованные или закрытые технологии, например, Cisco применяет технологию EtherChannel(разработанную в начале 1990-х годов компанией Kalpana), а также нестандартный протокол PAgP.

EtherChannel даёт возможность объединять от двух до восьми 100 Мбит/с, 1 Гбит/с или 10 Гбит/с портов Ethernet (все порты в канале должны иметь одинаковую скорость), работающих по витой паре или по оптоволокну, что позволяет достичь результирующей скорости до 80 Гбит/с. Дополнительно, от одного до семи портов могут быть неактивны и включаться в работу при обрыве соединения по одному из активных портов. При отсутствии резервных портов, трафик автоматически распределяется по всем активным соединениям.

Канал может устанавливаться между маршрутизаторами, коммутаторами и сетевыми адаптерами на сервере. Все сетевые адаптеры, являющиеся частью канала, получают один MAC-адрес, что делает канал прозрачным для сетевых приложений. Балансировка трафика между портами производится на

основе хэш-функции над MAC-адресом, IP-адресом или TCP и UDP портом источника или получателя. Таким образом, в некоторых неблагоприятных случаях, весь трафик может передаваться по одному физическому соединению.

При использовании протокола STP вместе с EtherChannel, все соединения в канале рассматриваются как одно логическое и BPDU посылается только по одному из них.

Агрегирование каналов в Cisco

Для агрегирования каналов в Cisco может быть использован один из трёх вариантов:

- LACP (Link Aggregation Control Protocol) стандартный протокол;
- PAgP (Port Aggregation Protocol) проприетарный протокол Cisco;
- статическое агрегирование без использования протоколов.

Так как LACP и PAgP решают одни и те же задачи (с небольшими отличиями по возможностям), то лучше использовать стандартный протокол. Фактически остается выбор между LACP и статическим агрегированием.

Статическое агрегирование:

Преимущества:

- не вносит дополнительную задержку при создании агрегированного канала или изменении его настроек;
- вариант, который рекомендует использовать Cisco.

Недостатки:

- нет согласования настроек с удаленной стороной. Ошибки в настройке могут привести к образованию петель.

Агрегирование с помощью LACP:

Преимущества:

- согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети;

- поддержка standby-интерфейсов позволяет агрегировать до 16ти портов, 8 из которых будут активными, а остальные в режиме standby.

Недостатком является дополнительная задержка при создании агрегированного канала или изменении его настроек.

Терминология и настройка

При настройке агрегирования каналов на оборудовании Cisco используется несколько терминов:

- EtherChannel — технология агрегирования каналов. Термин, который использует Cisco для агрегирования каналов;
- port-channel — логический интерфейс, который объединяет физические интерфейсы;
- channel-group — команда, которая указывает какому логическому интерфейсу принадлежит физический интерфейс и какой режим используется для агрегирования.

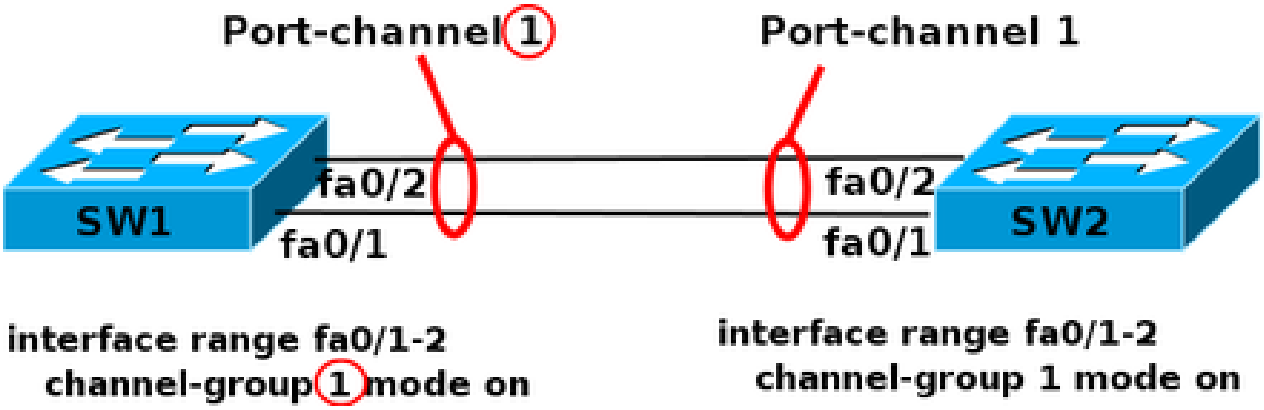

Рисунок 6 — Агрегирование каналов свич свич

Эти термины используются при настройке, в командах просмотра, независимо от того, какой вариант агрегирования используется (какой протокол, какого уровня EtherChannel).

На рисунке (рисунок 6), число после команды channel-group указывает какой номер будет у логического интерфейса Port-channel. Номера логических интерфейсов с двух сторон агрегированного канала не обязательно должны совпадать. Номера используются для того чтобы отличать разные группы портов в пределах одного коммутатора.

Общие правила настройки EtherChannel

LACP и PAgP группируют интерфейсы с одинаковыми:

- скоростью (speed);
- режимом дуплекса (duplex mode);
- native VLAN;
- диапазоном разрешенных VLAN;
- trunking status;
- типом интерфейса.

Настройка EtherChannel

Так как для объединения в EtherChannel на интерфейсах должны совпадать многие настройки, проще объединять их, когда они настроены по умолчанию. А затем настраивать логический интерфейс.

Перед объединением интерфейсов лучше отключить их. Это позволит избежать блокирования интерфейсов STP (или перевода их в состояние err-disable).

Для того чтобы удалить настройки EtherChannel достаточно удалить логический интерфейс. Команды channel-group удалятся автоматически.

Создание EtherChannel для портов уровня 2 и портов уровня 3 отличается:

- для интерфейсов 3го уровня вручную создается логический интерфейс командой interface port-channel;
- для интерфейсов 2го уровня логический интерфейс создается динамически.

Для обоих типов интерфейсов необходимо вручную назначать интерфейс в EtherChannel. Для этого используется команда channel-group в режиме настройки интерфейса. Эта команда связывает вместе физические и логические порты.

После того как настроен EtherChannel:

- изменения, которые применяются к port-channel интерфейсу, применяются ко всем физическим портам, которые присвоены этому port-channel интерфейсу;
- изменения, которые применяются к физическому порту влияют только на порт, на котором были сделаны изменения.

Синтаксис команды channel-group:

```
sw(config-if)# channel-group <channel-group-number> mode <<auto [non-silent] |
desirable [non-silent] | on> | <active | passive>>
```

Параметры команды:

- active — Включить LACP;
- passive — Включить LACP только если придет сообщение LACP;
- desirable — Включить PAgP;
- auto — Включить PAgP только если придет сообщение PAgP;
- on — Включить только Etherchannel.

Протокол STP

Spanning Tree Protocol (STP, протокол остовного дерева) — канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

Протокол работает на канальном уровне. STP позволяет делать топологию избыточной на физическом уровне, но при этом логически блокировать

петли. Достигается это с помощью того, что STP отправляет сообщения BPDU и обнаруживает фактическую топологию сети. А затем, определяя роли коммутаторов и портов, часть портов блокирует так, чтобы в итоге получить топологию без петель.

Для того чтобы определить какие порты заблокировать, а какие будут передавать данные, STP выполняет следующее:

- выбор корневого моста (Root Bridge);
- определение корневых портов (Root Port);
- определение выделенных портов (Designated Port).

Выбор корневого моста

Корневым становится коммутатор с наименьшим идентификатором моста (Bridge ID).

Только один коммутатор может быть корневым. Для того чтобы выбрать корневой коммутатор, все коммутаторы отправляют сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID.

В итоге только один коммутатор останется корневым и будет передавать BPDU.

Изначально Bridge ID состоял из двух полей:

- приоритет — поле, которое позволяет административно влиять на выборы корневого коммутатора. Размер — 2 байта;
- MAC-адрес — используется как уникальный идентификатор, который, в случае совпадения значений приоритетов, позволяет выбрать корневой коммутатор. Так как MAC-адреса уникальны, то и Bridge ID уникален, так что какой-то коммутатор обязательно станет корневым.

Определение корневых портов

Порт коммутатора, который имеет кратчайший путь к корневому коммутатору, называется корневым портом. У любого не корневого коммутатора может быть только один корневой порт. Корневой порт выбирается на основе меньшего Root Path Cost — это общее значение стоимости всех линков до корневого коммутатора. Если стоимость линков до корневого коммутатора совпадает, то выбор корневого порта происходит на основе меньшего Bridge ID коммутатора. Если и Bridge ID коммутаторов до корневого коммутатора совпадает, то тогда корневой порт выбирается на основе Port ID.

Определение назначенных портов

Коммутатор в сегменте сети, имеющий наименьшее расстояние до корневого коммутатора, называется назначенным коммутатором (мостом). Порт этого коммутатора, который подключен к рассматриваемому сегменту сети называется назначенным портом. Так же как и корневой порт выбирается на основе:

- меньшего Root Path Cost;
- меньшего Bridge ID;
- меньшего Port ID.

Протокол RSTP

Стандарт 802.1D для протокола связующего дерева (STP) был разработан в период, когда допустимым считалось восстановление соединения за время порядка минуты. После внедрения в среде локальных сетей коммутации уровня 3 мостовые соединения конкурируют с решениями с использованием маршрутизации, где такие протоколы, как протокол открытия кратчайшего маршрута первым (OSPF) и расширенный внутренний протокол маршрутизации шлюза (EIGRP), способны обеспечить запасной маршрут за меньшее время.

Для уменьшения времени сходимости мостовой сети исходная спецификация 802.1D была дополнена функциями Cisco Uplink Fast, Backbone Fast

и Port Fast. Недостатком является то, что эти механизмы являются запатентованными и им требуется дополнительная настройка.

Протокол быстрого связующего дерева (RSTP; IEEE 802.1w) можно рассматривать скорее как развитие стандарта 802.1D, а не как революционное его изменение. В основном терминология 802.1D остается той же. Большинство параметров остались неизменными, поэтому пользователи, знакомые с 802.1D, смогут быстро настроить новый протокол. В большинстве случаев производительность RSTP выше, чем у ненастроенных расширений, принадлежащих Cisco. 802.1w может функционировать для отдельных портов как 802.1D для взаимодействия с устаревшими мостами. При этом теряются преимущества, которыми обладает новый протокол.

Новая версия стандарта 802.1D, IEEE 802.1D-2004, включает стандарты IEEE 802.1t-2001 и IEEE 802.1w.

Роли портов

Теперь роль, назначенная определенному порту, является изменяемой. Роли корневого и назначенного порта остались, а роль блокирующего порта разделена на роли резервного и дополнительного портов. Алгоритм связующего дерева (STA) определяет роль порта в сети на основе блоков данных протокола моста (BPDU). Чтобы было проще, следует запомнить одну вещь — всегда можно сравнить любые два BPDU и решить, какой из них полезнее. Это основано на значении, хранящемся в BPDU и в некоторых случаях на порте, на который они были приняты. С учетом этого в данном разделе рассматриваются практические подходы к ролям портов.

Роли корневых портов (Root Port)

Порт, принимающий оптимальный блок BPDU по мостовому соединению, называется корневым. Этот порт является ближайшим к корневому мосту с позиции стоимости пути. Во всей сети с мостовыми подключениями STA выбирает один корневой мост (на каждую VLAN). Корневой мост передает самые оптимальные BPDU по сравнению с остальными мостами. Корне-

вой мост — это единственный мост в сети, у которого нет корневых портов. Все другие мосты получают BPDU хотя бы на один порт.

Роль назначенного порта (Designated Port)

Порт является назначенным, если он может передавать оптимальные BPDU в сегмент, к которому он подключен. Мосты 802.1D создают домен с мостовым соединением путем связывания различных сегментов (например, сегментов Ethernet). В указанном сегменте может быть только один путь к корневому мосту. При наличии двух мостов в сети возникает мостовая петля. Все мосты, связанные с указанным сегментом, прослушивают BPDU друг друга и согласуют мост, отправляющий лучшие BPDU, который становится назначенным мостом для этого сегмента. Соответствующий порт данного моста является назначенным.

Дополнительные и резервные роли портов

Эти две роли порта соответствуют состоянию блокирования стандарта 802.1D. Заблокированный порт определяется как порт, не являющийся выделенным или корневым. Заблокированный порт получает более полезные блоки данных BPDU, чем те, которые он посылал бы в свой сегмент. Следует помнить, что для сохранения блокирования порт должен получать BPDU. Эти две роли портов введены в RSTP со следующей целью:

Дополнительный порт получает более полезные BPDU от другого моста и порт остается заблокированным. Это показано на следующей схеме:

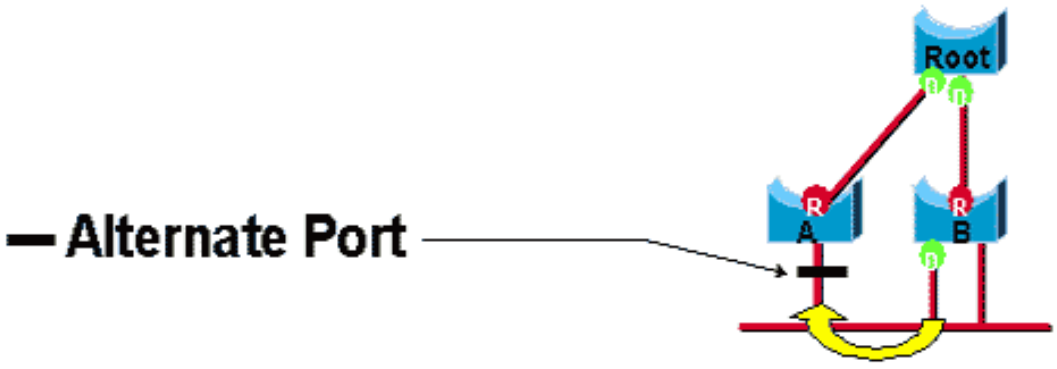

Рисунок 7 — Alternate Port

Резервный порт получает более полезные BPDU от этого же моста и порт остается заблокированным. Это показано на следующей схеме:

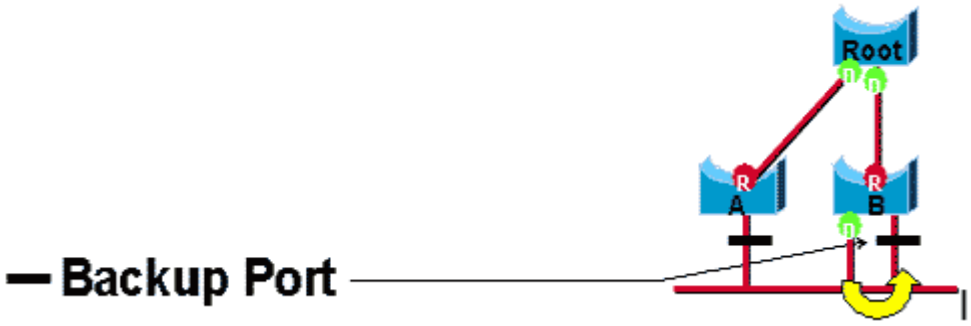

Рисунок 8 — Backup Port

Это различие уже подразумевалось в рамках стандарта 802.1D. Это является важным в работе функции UplinkFast Cisco. Обоснование этого заключается в том, что дополнительный порт предоставляет дополнительный путь к корневому мосту и, таким образом, может заменить корневой порт в случае его сбоя. Естественно, резервный порт обеспечивает резервное подключение к тому же сегменту и не может гарантировать резервирование подключения к корневому мосту. Поэтому он исключен из группы восходящих портов.

В результате RSTP рассчитывает конечную топологию для связующего дерева с помощью критериев, аналогичных 802.1D. В способе использования различных приоритетов мостов и портов не произошло абсолютно никаких изменений. В реализации Cisco для сбрасывающего состояния используется термин "блокирование". В версиях CatOS, начиная с 7.1, отображаются состояния прослушивания и обучения. Это дает даже больше информации о порте, чем требуется стандартом IEEE. Однако новое свойство заключается в том, что теперь между ролью, определяемой протоколом для порта, и его текущим состоянием существует различие. Например, порт может быть назначенным и заблокированным одновременно, и теперь такая ситуация является допустимой. Поскольку такая ситуация наблюдается очень небольшой отре-

зок времени, это просто значит, что порт находится в состоянии перехода к состоянию назначенного пересылающего порта.

VLAN

VLAN (аббр. от англ. Virtual Local Area Network) — виртуальная локальная компьютерная сеть. Группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности, в частности как средство борьбы с ARP-spoofing'ом.

Гибкое разделение устройств на группы.

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

Уменьшение количества широковещательного трафика в сети.

Каждый VLAN — это отдельный широковещательный домен. Например, коммутатор — это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же

VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

Увеличение безопасности и управляемости сети.

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Обозначение членства в VLAN

Для этого существуют следующие решения:

- по порту (англ. port-based, 802.1Q): порту коммутатора вручную назначается одна VLAN. В случае, если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько сетевых коммутаторов), то этот порт должен быть членом транка. Только одна VLAN может получать все пакеты, не отнесённые ни к одной VLAN (в терминологии 3Com, Planet, D-Link, Zyxel, HP — untagged, в терминологии Cisco, Juniper — native VLAN). Сетевой коммутатор будет добавлять метки данной VLAN ко всем принятым кадрам, не имеющим никаких меток. VLAN, построенные на базе портов, имеют некоторые ограничения;
- по MAC-адресу (MAC-based): членство в VLANe основывается на MAC-адресе рабочей станции. В таком случае сетевой коммутатор имеет таблицу MAC-адресов всех устройств вместе с VLANами, к которым они принадлежат;
- по протоколу (Protocol-based): данные 3-4 уровня в заголовке пакета используются, чтобы определить членство в VLANe. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость

уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети;

- методом аутентификации (англ. authentication based): устройства могут быть автоматически перемещены в VLAN, основываясь на данных аутентификации пользователя или устройства при использовании протокола 802.1x.

VLAN в Cisco

В устройствах Cisco, протокол VTP (англ. VLAN Trunking Protocol) предусматривает VLAN-домены для упрощения администрирования. VTP также выполняет «чистку» трафика, направляя VLAN трафик только на те коммутаторы, которые имеют целевые VLAN-порты (функция VTP pruning). Коммутаторы Cisco, в основном, используют протокол 802.1Q Trunk вместо устаревшего проприетарного ISL (англ. Inter-Switch Link) для обеспечения совместимости информации.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Native VLAN — это параметр каждого порта, который определяет номер VLAN, его получают все непомеченные (untagged) пакеты.

В Cisco используется следующая терминология портов:

- access port — порт, принадлежащий одному VLAN’у и передающий не тегированный трафик. По спецификации cisco, access порт может принадлежать только одному VLAN’у, по умолчанию это первый (не тегированный) VLAN. Любой кадр, который проходит через access порт, помечается номером, принадлежащим этому VLAN’у;
- trunk port — порт, передающий тегированный трафик одного или нескольких VLAN’ов. Этот порт, наоборот, не изменяет тег, а лишь пропускает кадры с тегами, которые разрешены на этом порту.

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.

Режимы интерфейса (режим по умолчанию зависит от модели коммутатора):

- auto — Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. То есть, если порты на обоих концах находятся в режиме «auto», то trunk применяться не будет;
- desirable — Порт находится в режиме «готов перейти в состояние trunk»; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto);
- trunk — Порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим;
- nonegotiate — Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим «не-cisco» оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk’a.

По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

Преимущества

- облегчается перемещение, добавление устройств и изменение их соединений друг с другом;
- достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне;
- уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;
- сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений;
- предотвращение широковещательных штормов и предотвращение потерь.

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ ПО ТЕМЕ «ТЕХНОЛОГИИ КАНАЛЬНОГО УРОВНЯ МОДЕЛИ OSI В GNS3»

В подготовке IT специалистов очень важна практическая часть работы, но не всегда есть возможность выполнения практической работы на реальном оборудовании. Есть несколько кроссплатформенных симуляторов выпускаемые компанией Cisco. Но одно из них платное, а другое поддерживает не все функции оборудования. Поэтому данный лабораторный практикум выполняется в свободно распространяемом кроссплатформенном симуляторе GNS3.

Методическое обеспечение для подготовки специалиста в определенной области деятельности — это совокупность нормативно-методических разработок, специально предназначенных для решения задач, связанных с областью деятельности будущего специалиста. Основная его функция — определённый способ осуществления практической или теоретической деятельности; алгоритм конструирования и организации деятельности. Обычно понятием методического руководства обозначают некую осознанную систему действий, приводящих к определённым результатам. Конечная цель методического обеспечения — оснащение учащихся и преподавателей передовой методикой и на этой основе обеспечение высокого уровня обучения, соответствующего потребностям общества.

2.1 Структура и программная среда разработки лабораторного практикума

Лабораторный практикум «Технологии канального уровня модели OSI в GNS3» включает:

Теоретические сведения необходимые для настройки и работы с некоторыми технологиями канального уровня.

Лабораторные работы для учащихся, которые обучаются по дисциплине компьютерные коммуникации и сети.

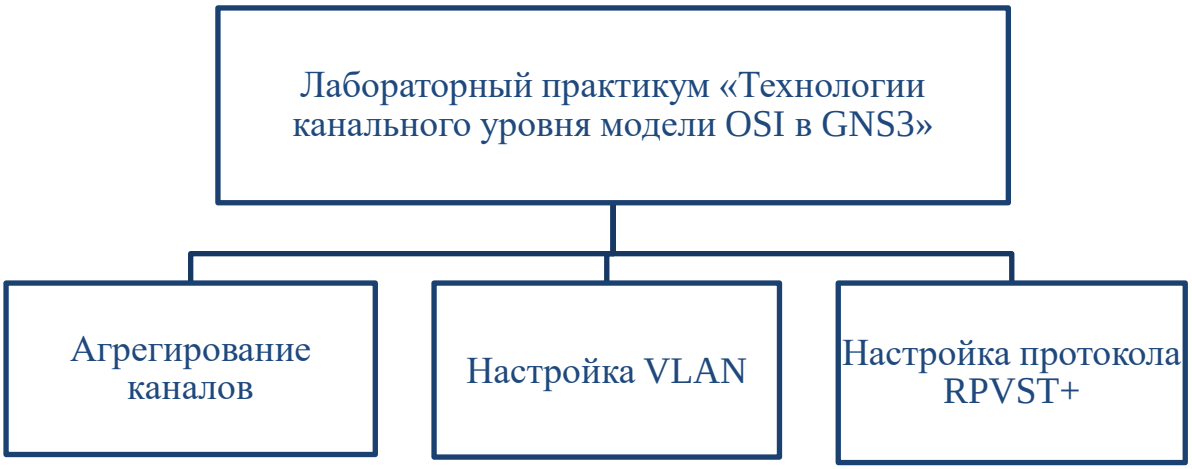

Рисунок 9 — Структура лабораторного практикума

Структура лабораторного практикума «Технологии канального уровня модели OSI в GNS3» представлена на рисунке 9.

Для создания и форматирования руководства использовался текстовый процессор MS Word 2013 (рисунок 10). Возможности процессора полностью соответствуют требованиям: редактирование и форматирование текста, вставка и оформление графических изображений, создание автоматического оглавления, создание и настройка гиперссылок.

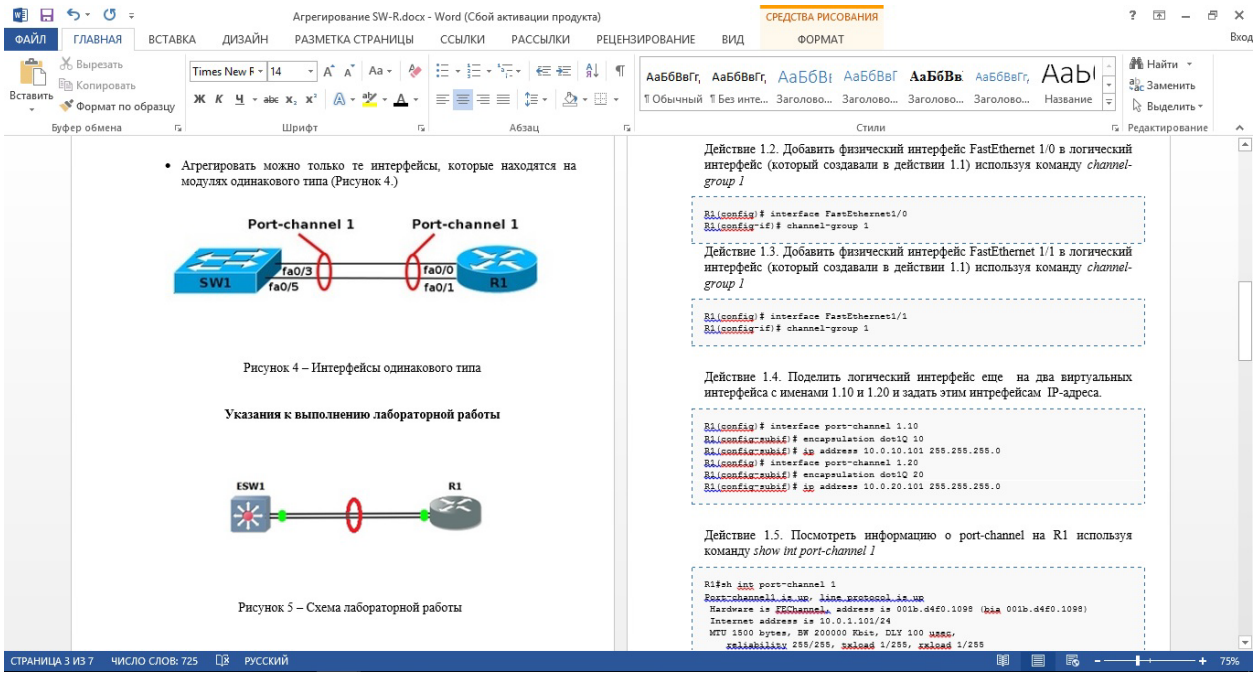

Рисунок 10 — Отображение электронного пособия в текстовом процессоре MS Word

Итоговый результат руководства сохранен в формате PDF. MS Word позволяет сохранять документы в этом формате, а также предоставляет возможность настроить дополнительные параметры

Достоинства формата PDF:

- кроссплатформенность. Возможность работать с документом в любой операционной системе;
- низкая требовательность к печатающим устройствам. Документ печатается без искажений на принтерах любого класса;
- высокая компактность. Формат позволяет работать со многими алгоритмами сжатия данных;
- совместимость с мультимедийным контентом. PDF-документы позволяют присоединять мультимедийные и гипертекстовые элементы, а также допускают предварительный просмотр страниц;
- возможность настройки уровня безопасности. Например, блокировка открытия PDF-документа, его печати или же редактирования.

Для работы с документом в формате PDF можно использовать разные программы:

- программы просмотра, печати и комментирования документов в формате PDF Adobe Acrobat Reader, Foxit Reader, Sumatra PDF;
- браузеры, например, Opera, Google Chrome, Mozilla Firefox.

На рисунке 11 представлен внешний вид руководства в браузере Google Chrome.

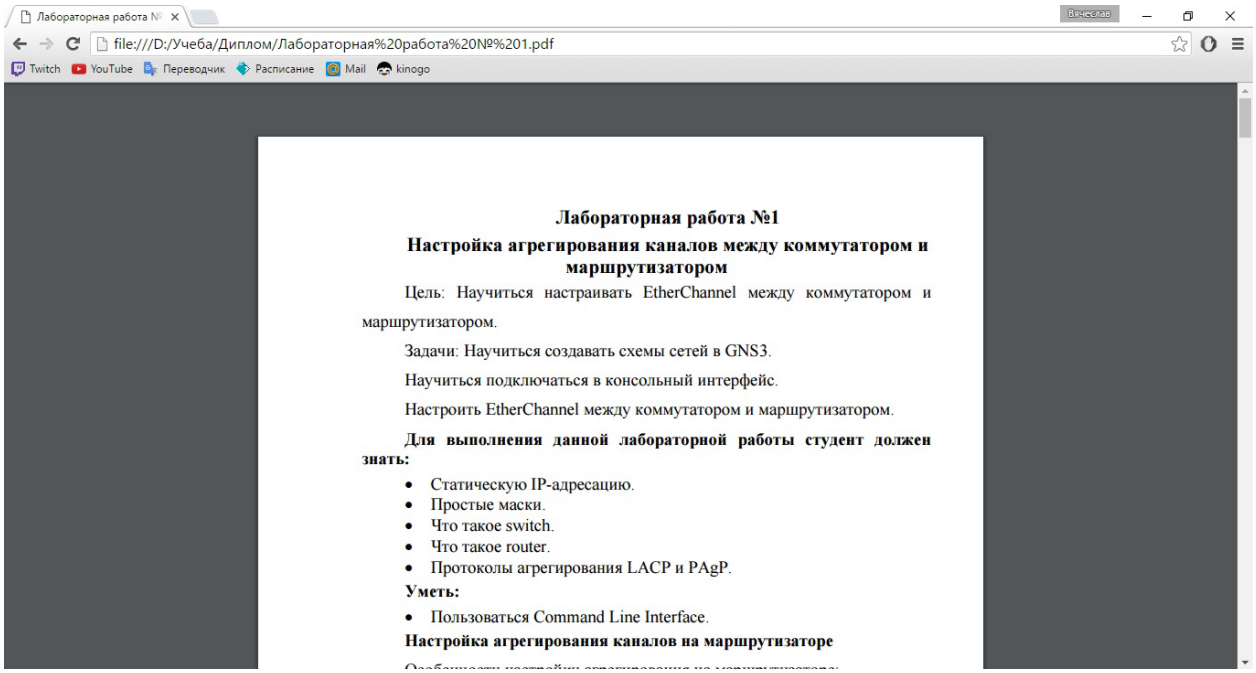

Рисунок 11 — Просмотр руководства в браузере Google Chrome

Чтобы реализовать систему навигации, необходимо при сохранении документа в формате PDF выбрать параметр «Создать закладки, используя заголовки» в диалоговом окне Параметры (рисунок 12).

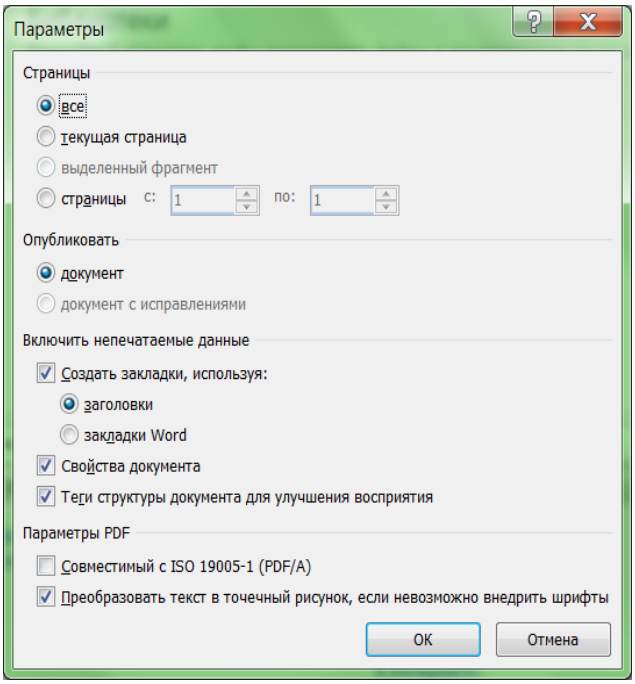

Рисунок 12 — Настройка параметров при сохранении в формате PDF

В разделе «Теоретические сведения» рассмотрены наиболее важные теоретические сведения необходимые для успешного выполнения лабораторных работ и контрольных заданий.

В данном разделе рассмотрены такие темы как:

1. Агрегирование каналов.
2. Протокол STP.
3. VLAN.

2.2 Описание лабораторных работ лабораторного практикума «Технологии канального уровня модели OSI в GNS3»

К концу обучения учащийся должен уметь работать с оборудованием компании Cisco System как в симуляторе, так и на реальном оборудовании. Для обучения студентов работе с оборудованием Cisco будет применяться графический симулятор сети GNS3.

Cisco Systems является одним из мировых лидеров по производству оборудования для создания эффективных сетевых сред. Компания поставляет на рынок высокотехнологичного оборудования серверы, сетевое оборудова-

ние, коммутаторы и другое оборудование, позволяющее развертывать современные и производительные IT-инфраструктуры.

Они предлагают широкий ассортимент оборудования. На сайте можено найти как самые новые модели оборудование, так и устройства снятые с производства, а также комплектующие к ним.

Cisco System представляют следующее оборудование:

Серверы Cisco UCS — основной элемент новой инфраструктурной платформы, позволяющей объединить вычислительные мощности, инструменты управления, виртуализации, устройства хранения в единую структуру.

Сетевое оборудование Cisco, предоставляющее пользователю возможность развернуть максимально эффективную инфраструктуру, демонстрирующую высочайшие показатели функциональности и надежности.

Коммутаторы Cisco — современные устройства, с высоким уровнем производительности. Коммутаторы Cisco обладают отличными возможностями масштабирования, в соответствии с потребностями сетевых инфраструктур различного размера.

Маршрутизаторы Cisco, пользующиеся стабильным спросом у организаций различного уровня. Эти устройства помогают построить максимально эффективную и производительную сетевую инфраструктуру современного предприятия для решения сложных задач, постоянно возникающих перед современными организациями.

Точки доступа Cisco обеспечивают возможность организации хорошо защищенных, надежных и управляемых беспроводных сетей. Точки доступа Cisco совместимы с широким спектром клиентских устройств, благодаря чему пользователь может развернуть на их основе удобную беспроводную инфраструктуру.

Телекоммуникации Telepresence — это современная платформа, обеспечивающая уникальные средства коммуникаций, и используется для наиболее эффективного решения бизнес задач и личного общения.

GNS3 — Graphical Network Simulator — это графический симулятор сети, который позволяет смоделировать виртуальную сеть из маршрутизаторов и виртуальных машин. Незаменимый инструмент для обучения и тестов. Работает практически на всех платформах. В зависимости от аппаратной платформы, на которой будет использоваться GNS3, возможно построение комплексных проектов, состоящих из маршрутизаторов Cisco, Cisco ASA, Juniper, а также серверов под управлением сетевых операционных систем. При отсутствии возможности получить доступ к реальному оборудованию, GNS3 станет практически полноценной лабораторией. Кроме того, лабораторные работы, выполняемые в GNS3, могут стать дополнением к занятиям в реальной лаборатории.

Одной из самых интересных особенностей GNS3 является возможность соединения проектируемой топологии с реальной сетью. Это дает просто уникальную возможность проверить на практике какой-либо проект, без использования реального оборудования. Использование WireShark позволяет провести мониторинг трафика внутри проектируемой топологии, что дает дополнительную информацию для понимания изучаемых технологий.

GNS3 бесплатен. Это открытое программное обеспечение, и любой желающий может скачать его с официального сайта проекта в разделе Download. На данный момент есть версии для Linux, MS Windows XP и Windows 7, а также для MacOS.

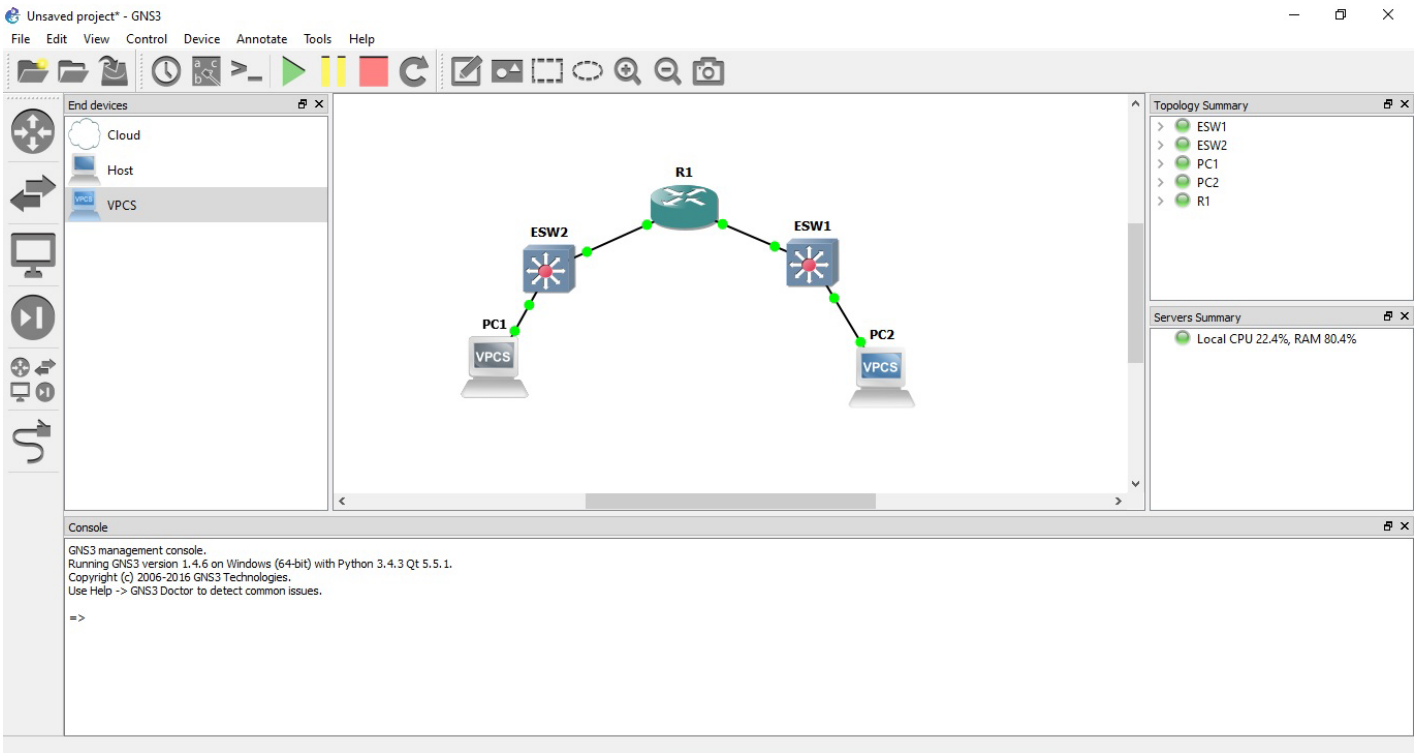

Рисунок 13 — GNS3

Лабораторная работа № 1.

В первом задании лабораторной работы производится запуск симулятора GNS3 и подготовка схемы, представленной в лабораторной работе (рисунок 14).

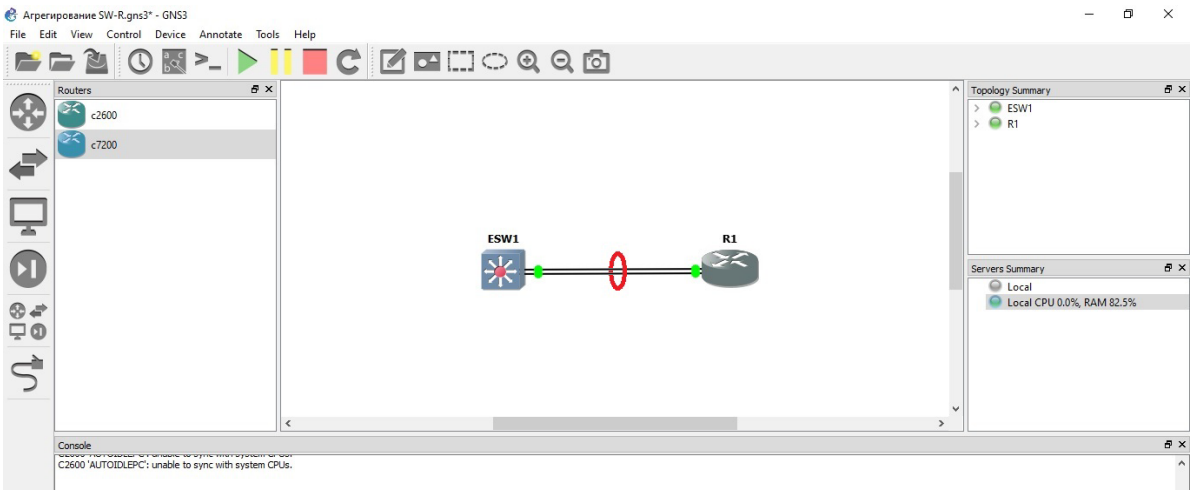

Рисунок 14 — Схема лабораторной работы

Во время выполнения второй части лабораторной работы требуется запустить на роутере режим консоли, создать логические игтерфейсы, присвоить им IP-адреса, добавить физические интерфейсы в созданные ранее логические и посмотреть с помошью определенной команды проделаную работы.

В третьей части лабораторной работы производится запуск консоли на коммутаторе, указывается к какому логическому интерфейсу пренадлежат физические интерфейсы, указывается режим агрегирования и нужно сделать порты транковыми, в конце посмотреть информацию о EtherChannel на коммутаторе.

В задании четыре требуется произвести настройку агрегирования каналов с протоколом LACP между двумя коммутаторами

В задании пять нужно произвести настройку агрегирования каналов с протоколом PAgP между двумя коммутаторами

В конце лабораторной работы требуется выполнить контрольное задание и ответить на вопросы.

Лабораторная работа № 2.

Изначально в задании один лабораторной работы номер два требуется запустить симулятора GNS3 и подготовить схему, представленную в лабораторной работе (рисунок 15). В подготовку схему входит:

- создание топологии сети;
- установка IP-адресации.

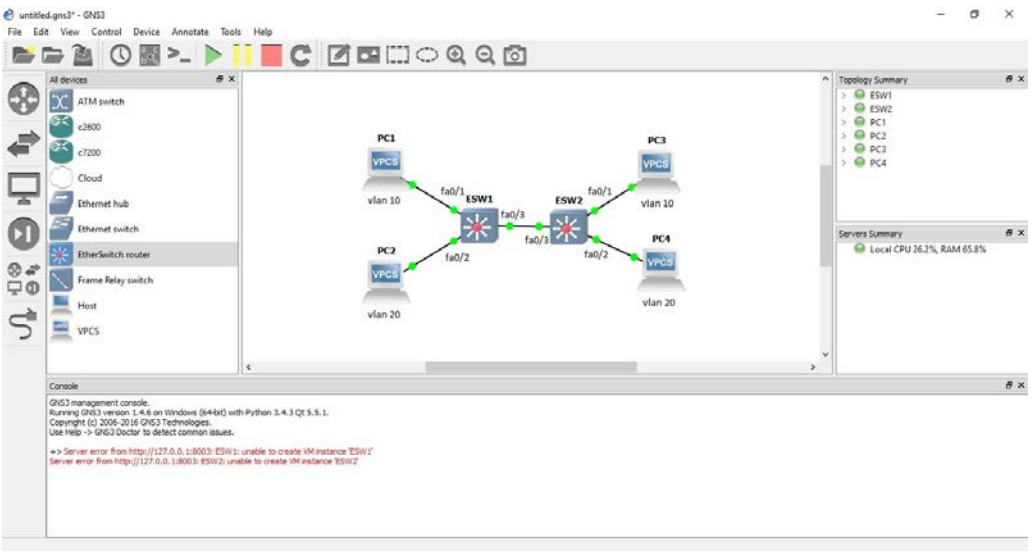

Рисунок 15 — Схема лабораторной работы

Во второй части первого задания производится настройка первого коммутатора. Первым делом нужно зайти в консоль на коммутаторе. Затем создать VLAN, задать ему имя, перейти в настройки интерфейса, присвоить интерфейс определенному VLAN и задать режим работы этого интерфейса. В третьей части первого задания нужно настроить коммутатор под номером два аналогично предыдущему.

В задании два требуется настроить Native VLAN.

В первой части второго задания нужно воспроизвести схему, приведенную на рисунке 16.

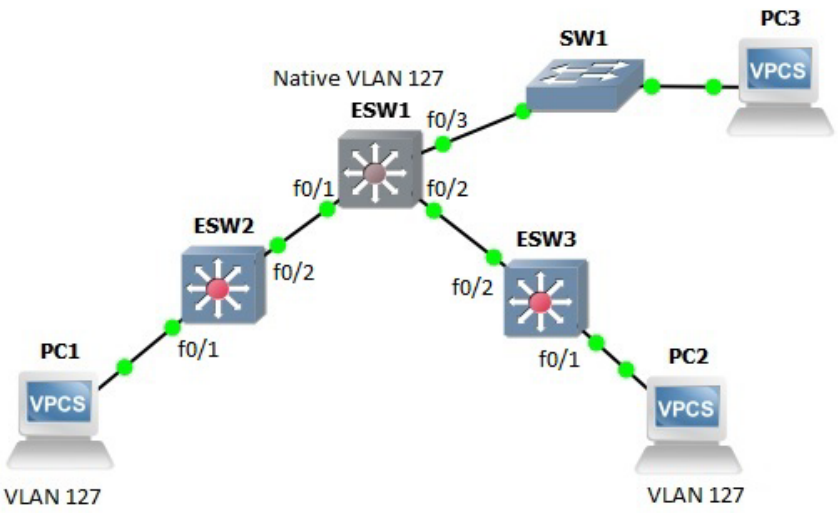

Рисунок 16 — Схема задания два

Во второй части задания два производится настройка коммутатора под номером два: создаются виртуальные локальные сети и настраиваются интерфейсы.

В третьей части задания настраиваться коммутатор номер три. Настройка такая же как на коммутаторе два.

В четвертой части нужно настроить коммутатор номер один, на нем так же создается виртуальная локальная сеть и настраиваются интерфейсы.

В конце лабораторной работы требуется выполнить контрольное задание и ответить на вопросы.

Лабораторная работа № 3.

Первым действием производится запуск симулятора GNS3 и подготовка схемы, представленной в лабораторной работе (рисунок 17).

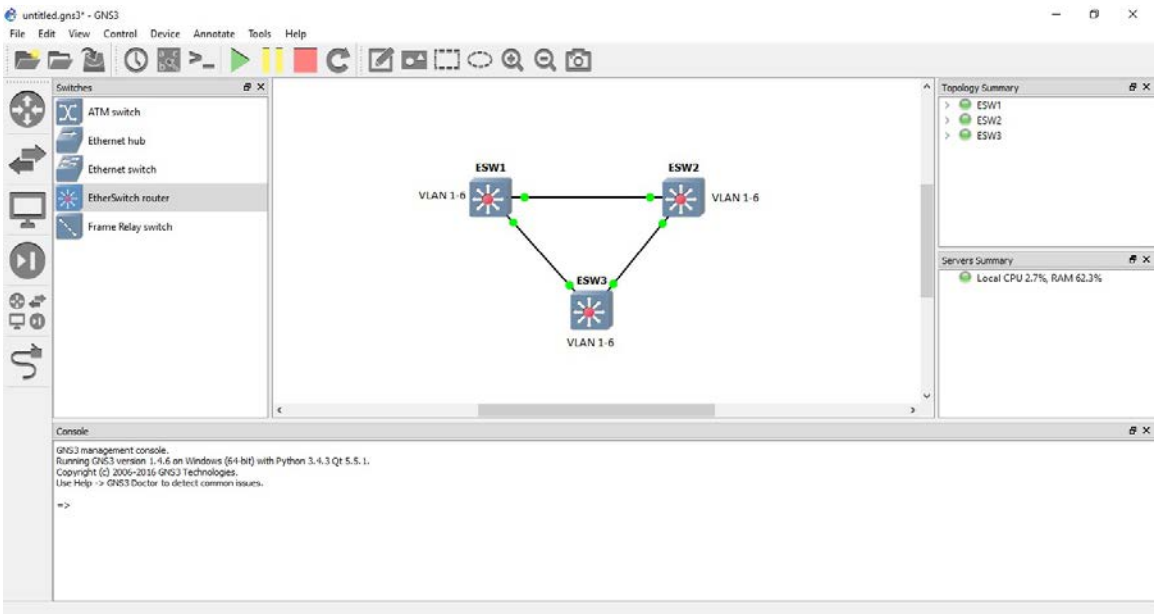

Рисунок 17 — Схема лабораторной работы

Во второй части лабороторной работы производится настройка первого коммутатора. Изначально нужно запустить режим консоли на коммутаторе. Затем переходим к настройке RPVST+, здесь выставляем таймер на рассылку пакетов hello, таймер перехода режима портов в другое состояние и устанавливаем время максимального действия остовного дерева. Затем

переходим к настройке интерфейсов на коммутаторе, задаем приоритет интерфейсу и различные дополнительные функции.

В третьей части лабораторной работы настраиваем коммутатор номер два. В целом настройки идентичны, отличаютя лишь тем, что не нужно выставлять тайминги, так как первый коммутатор «раскажет» о них.

В четвертой части лабораторной работы так же настраиваем коммутатор, только уже под номером три. Здесь настройки идентичны настройкам на втором коммутаторе.

В конце лабораторной работы требуется выполнить контрольное задание и ответить на вопросы.

ЗАКЛЮЧЕНИЕ

В данной выпускной квалификационной работе рассматривались вопросы и проблемы, связанные с канальными технологиями модели OSI, работой в симуляторах по постройке и администрированию компьютерных сетей.

По результатам проведенных исследований можно сделать определенные выводы:

- канальные технологии подразумевают работу не только на оборудовании канального уровня, но и сетевого;
- симулятор GNS3 является отличным решения для построения и настройки компьютерной сети;
- благодаря использованию технологии VLAN удается существенного сократить расходы на расширение сетей;
- с помощью технологии RPVST+ можно избежать широковещательного шторма;
- агрегация каналов позволяет увеличить пропускную способность и надежность соединения.

Разработанный лабораторный практикум включает в себя лабораторные работы по выполнению настройки технологий канального уровня модели OSI на сетевом оборудовании в симуляторе GNS3. Лабораторный практикум будет использоваться для проведения занятий по дисциплине компьютерные коммуникации и сети «РГППУ».

Цель выпускной квалификационной работы достигнута, поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Альтман Е. А. Компьютерные сети на базе оборудования фирмы Cisco [Текст] / Е. А. Альтман. — Омский гос. ун-т путей сообщения. — Омск: 2007. — 32 с.

2. Кузнецов М. А. Современные технологии и стандарты подвижной связи [Текст] / М. А Кузнецов, Рыжков А. Е. — СПб. : Линк, 2014. — 405 с.

3. Коммутаторы консоли, переключатели, удлинители [Электронный ресурс]. — Режим доступа: http://born–spb.ru /catalog/kommutat ory–konsoli–kvm.html (дата обращения: 17.11.2015).

4. Новиков Ю. В. Основы локальных сетей. Курс лекций: учебное пособие [Текст] / Ю. В. Новиков, С. В. Кондратенко. — М.: Интернет — Ун-т Информ. Технологий, 2014. — 337 с.

5. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов [Текст] / В. Г. Олифер, Н. А. Олифер. — СПб. : Питер, 2013. — 334 с.

6. Олифер В. Г. Базовые технологии локальных сетей [Текст] / В. Г. Олифер, Н. А. Олифер. — СПб. : Питер, 2013. — 434 с.

7. Таненбаум Э. С. Компьютерные сети [Текст] / Э. С. Таненбаум. — СПб. : Питер, 2012. — 992 с.

8. Финогеев А. Г. Сетевые технологии: Учебное пособие 3 часть. Углубленный уровень подготовки [Текст] / А. Г.Финогеев, А. С. Бождай. — Пенза, 2013. — 192 с.

9. Cisco Packet Tracer [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/ Cisco Packet Tracer (дата обращения: 25.05.2016).

10. Эрганова Н. Е. Методика профессионального обучения [Текст]: учеб. пособие / Н. Е. Эрганова. — М.: Издательский центр «Академия», 2008. — 160 с.

11. Эрганова Н. Е. Практикум по методике профессионального обучения [Текст]: учеб. пособие / Н. Е. Эрганова. — Екатеринбург: Изд-во Рос. гос. проф.-пед.ун-та, 2011. — 89 с.

12. Эрганова Н. Е. Практикум по педагогическим технологиям [Текст]: учеб. пособие / Н. Е. Эрганова. — Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2011. — 50 с.

13. Агрегирование каналов [Электронный ресурс] — Режим доступа: ru.wikipedia.org/wiki/Агрегирование_каналов (дата обращения: 25.05.2016);

14. Xgu [Электронный ресурс] — Режим доступа: http://xgu.ru/ (дата обращения: 25.05.2016).

15. Cisco [Электронный ресурс] — Режим доступа: http://www.cisco.com (дата обращения: 25.05.2016).

16. Хабраха́бр [Электронный ресурс] — Режим доступа: http://habrahabr.ru/post/134892/ (дата обращения: 25.05.2016).

17. learningnetwork.cisco [Электронный ресурс] — Режим доступа: http:// learningnetwork.cisco.com (дата обращения: 25.05.2016).

18. ipnet4you [Электронный ресурс] — Режим доступа: http://ipnet4you.ru/ (дата обращения: 25.05.2016).

19. ciscolab [Электронный ресурс] — Режим доступа: http://www.ciscolab.ru/ (дата обращения: 25.05.2016).

20. ccnastepbystep.blogspot [Электронный ресурс] — Режим доступа: http://ccnastepbystep.blogspot.ru/ (дата обращения: 25.05.2016).

21. Уэнделл Одом Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide [Текст] / Уэнделл Одом. — Вильямс, 2015. — 912 с.

22. Уэнделл Одом Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация [Текст] / Уэнделл Одом. — Вильямс, 2015. — 736 с.

23. Уэнделл Одом Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822 [Текст] / Уэнделл Одом. — Вильямс, 2015. — 427 с.

24. Уэнделл Одом Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640-816 [Текст] / Уэнделл Одом. — Вильямс, 2013. — 752 с.

25. Тодд Лэммл CCNA Cisco Certified Network Associate Study Guide [Текст] / Тодд Лэммл. — SYBEX Inc, 2011. — 864 с.

26. Тодд Лэммл, Кевин Хейлз CCNP. Настройка коммутаторов. Учебное руководство [Текст] / Тодд Лэммл, Кевин Хейлз. — Лори, 2015. — 464 с.

27. Тодд Лэммл CCNA: Cisco Certified Network Associate: Review Guide [Текст] / Тодд Лэммл. — Sybex, 2011. — 360 с.

28. Dale Liu Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit [Текст] / Dale Liu. — Syngress, 2009. — 848 с.

29. Richard Deal Cisco CCNA Cisco Certified Network Associate: Study Guide [Текст] / Dale Liu. — McGraw-Hill, 2011. — 1040 с.

30. Dale Liu Cisco Router and Switch Forensics [Текст] / Dale Liu. — Syngress, 2010. — 528 с.

ПРИЛОЖЕНИЕ

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
направление 44.03.04 Профессиональное обучение (по отраслям)
профиль «Энергетика»
профилизация «Компьютерные технологии автоматизации и управления»

УТВЕРЖДАЮ
Заведующий кафедрой
_____Н. С. Толстова
«____»_____2016 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента 4 курса курса, группы КТэ-401 Паньшина Вячеслава Евгеньевича

1. Тема Лабораторный практикум «Технологии канального уровня модели OSI в GNS3» утверждена распоряжением по институту от 23.03.2016 г. № № 57..

2. Руководитель Венков Сергей Сергеевич, старший преподаватель кафедры ИС.

3. Место преддипломной практики Учебно-технический центр ООО «Омега-1», г. Екатеринбург

4. Исходные данные к ВКР В. Г. Олифер, Н.В. Олифер «Компьютерные сети. Принципы, технологии, протоколы», Э. Таненбаум, Д. Уэзеролл «Компьютерные сети».

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
Проведен обзор и анализ литературных и интернет-источников.
Рассмотрены программные симуляторы для построения и настройки компьютерных сетей.
На основе анализа рабочей программы дисциплины «Компьютерные коммуникации и сети» спроектированы лабораторные работы.
Спроектированные работы объединены в методические указания к лабораторным работам и реализованы в формате .pdf.
6. Перечень демонстрационных материалов
Презентация, созданная в PowerPoint 2013

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	11.03.2016	15	
2	Выполнение работ по разрабатываемым вопросам их изложение в выпускной работе:			
	Выполнение и оформление теоретического раздела ВКР	22.03.2016	20	
	Работа над практическим разделом	04.04.2016	10	
	Выполнение и оформление практического раздела ВКР	22.04.2016	10	
	Работа над методическим разделом	02.05.2016	15	
	Выполнение и оформление методического раздела ВКР	12.05.2016	10	
3	Оформление текстовой части ВКР	26.05.2016	5	
4	Выполнение демонстрационных материалов к ВКР	30.05.2016	5	
5	Нормоконтроль	03.06.2016	5	
6	Подготовка доклада к защите в ГЭК	10.06.2016	5	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ *Задание получил* _____
подпись дата подпись студента дата

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Паньшина В. Е. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Паньшина В. Е. к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от 08.06.2016 №15)

Заведующий кафедрой _____ _____
подпись дата